The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/23/2019

SUBJECT:
Multiple Vulnerabilities in Microsoft Internet Explorer and Microsoft Defender Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer and Microsoft Defender, the most severe of which could allow for code execution. Microsoft Internet Explorer is a web browser available for Microsoft Windows. Microsoft Defender is an anti-virus component of Microsoft Windows. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining local system account privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are reports of CVE-2019-1367 being actively exploited in the wild.

SYSTEMS AFFECTED:
- Internet Explorer 9, 10, 11
- Microsoft Forefront Endpoint Protection 2010
- Microsoft Security Essentials
- Microsoft System Center 2012 Endpoint Protection
- Microsoft System Center 2012 R2 Endpoint Protection
- Microsoft System Center Endpoint Protection
- Windows Defender

RISK:
Government:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer and Microsoft Defender, the most severe of which could allow for arbitrary code execution:

- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2019-1367)
- A denial of service vulnerability exists when Microsoft Defender improperly handles files. An attacker could exploit the vulnerability to prevent legitimate accounts from executing legitimate system binaries. (CVE-2019-1255)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1255
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

ZDNet:
https://www.zdnet.com/article/microsoft-releases-out-of-band-security-update-to-fix-ie-zero-day-defender-bug/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1255
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1367

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov